

2.5.3. 教育活動概要

(a) 卒業論文概要

鷹嘴 将彦	近年、クラウドコンピューティング技術やスマートフォンやタブレット型PC の普及による、インターネットトラフィック量の急激な増加が社会的な問題となっている。これに伴い、通信機器数の増加や通信機器の高機能化による、消費電力量の増加も懸念されている。2025 年におけるネットワーク機器の消費電力量は2006 年の約13 倍になると予測されており、IT 機器全体の消費電力量の約43 %を占める値となっている。よって、ネットワークの省電力化は重要な課題であると言える。そこで本研究では、ネットワークトラフィック量の変化に応じてルーティングを行う機器の台数を増減し、必要のない機器をスリープさせることによってネットワーク全体の消費電力量を減少させる手法を提案した。具体的には、新たなネットワーク制御技術であるOpenFlow を用いることでネットワーク全体のトラフィック量の把握や機器のスリープ判断、ルートの変更作業を集中的に管理し、スループットを向上させたルーティングアルゴリズムを提案した。更に、評価実験により省電力効果とスループットを評価し、本提案手法の有効性を示した。
吉田 優介	Social Networking Service (SNS)は、人と人とのつながりの促進・サポートを目的としたコミュニティ型のWebサービスであり、近年では様々な種類のSNSが存在している。インターネットの普及に伴い、SNSの会員数は年々増加傾向にあり、今後ますます発展していくと考えられる。しかし、SNSの普及に伴って、SNSユーザ自身の発言内容から個人が特定されてしまうという問題が発生している。現在、この問題への効果的な対策は存在せず、ユーザの意識に委ねられるのみである。そこで本論文では、該当する発言を“間接的有害発言”と定義し、間接的有害発言検出のための手法を提案した。この提案手法では、SNSユーザの発言を、形態素解析、独自に定義した文脈定義文、独自に構築したユーザ単語辞書の3つの工程で分類する。この手法を適用したシステムを構築し、適合率・再現率・F値の3つの指標を用いて、間接的有害発言の検出精度について評価を行った。
横田 達也	従来より、論文盗用の問題が絶えず発生している。論文盗用は、文章のみをコピーして行われるため、文章自体へ対策を行わなければならない。この問題を解決する手段として辞書変換法での文章への電子透かしが挙げられる。しかし、過去の方法では文章に違和感が生じ文章が変更される可能性があり、電子透かしとして機能しない。本論文では、変換後意味がほとんど変化しない接続詞および副詞に着目し、文章の違和感を解消した新たな辞書変換の方法を示した。また、比較実験によりその有効性を検証した。
菊池 雄大	近年、コンピュータ犯罪の対象としてスマートフォンを狙う攻撃が増加している。攻撃手法として人間の心理や行動を利用するものが主であり、機械的な対策だけでは対処が困難である。そのため、ユーザ自らの対処が必要になるが、実際の場面に直面した場合の行動を想起し辛い。これらを解決するため、GBS 理論に基づいた教材の開発が行われているが、いくつか問題があるため、本研究ではそれらの解決方法の提案を行った。

益子 純平	近年増加傾向にあるタブレット PC における個人認証方式としては安全性と記憶保持性の両立が困難な従来の文字列パスワード方式が広く採用されている。マルチタッチスクリーンを利用した認証手法が提案されているが安全性に問題があり評価もなされていない。そこで本研究では既存手法の問題点を解決するため、使用できる指の本数を増加させ、マルチタッチの特徴を引き出して安全性を確保する個人認証手法を提案した。
-------	---

(b) 博士(前期)論文概要

野地 脩宏	<p>近年、インターネットでは、知的財産を大企業から窃取することを目的とする標的型攻撃や、標的の友人関係に忍びこむソーシャルネットワーク攻撃等のセキュリティ脅威が著しく増加している。これを受け、インターネットのトラフィックを観測することで、最新の脅威活動を早期に発見し、脅威活動の注意喚起・予防情報の提供を行うことを目的とした、インターネット観測システムの運用が行われている。</p> <p>しかし、既存の観測システムにおいて公開されている情報は、システム設置者によって解析が行われた後の情報のみであり、限定された情報である。よって、利用者が自身の環境・目的に合致した情報を得られない場合がある。また、固定された複数の観測点により構成されているため、観測点が発見され、回避される可能性がある。</p> <p>そこで筆者が所属する研究室では、このような問題点を考慮した、分散型インターネット観測システムABLA (Agent Based Log Analyzing System) の研究・開発を進めている。ABLAは、Peer-to-Peerによりネットワークを構築し、ABLA利用者同士が観測点となり、観測情報を提供し合う。また、モバイルエージェント（以下エージェント）が各観測点を移動し、観測情報の結果を収集することで、各観測点の匿名化を図るとともに、トラフィック量・処理量を抑えている。</p> <p>しかしながら、既存のABLAエージェントの移動手法では、観測情報の収集対象を隣接ノードのみとし、近隣のノードから優先的に観測情報の収集を行っていることから、利用者の要求をより良く満たす観測情報を見逃す可能性がある。この問題点から、従来のABLAは、利用者の要求に対する観測情報の収集が十分ではないと言える。</p> <p>そこで本論文では、まず、ABLAで用いられているモバイルエージェントの以下の3点からなる移動戦略を提案した：</p> <ol style="list-style-type: none"> 1) ノード情報の伝達による他ノード情報の獲得、 2) ノードの重み付け評価による移動先候補の選出、 3) 検索エージェントによる移動先ノードの決定。 <p>最後に、既存のインターネット観測システム、動的観測点を持つ従来のABLAシステム、本提案手法を適用したABLAシステム、これらの観測情報の収集を比較することで、本提案の有効性を評価し、観測情報のより柔軟な収集が可能な観測システムを実現した。</p>
-------	---

成田 匡輝	<p>インターネット技術の急速な発展に伴い、サイバー犯罪の増加が深刻な問題となっている。特にサービス拒否攻撃やマルウェアによる攻撃などは、攻撃を受けた企業にとって致命的な経済的損失となりうる。このことから、ネットワーク管理者は、常に自らの管理するネットワークを様々な攻撃から守るため、最新の攻撃動向に関する情報を入手しておく必要がある。また近年では、自らの管理するネットワークから攻撃者を輩出することにも厳しい目が向けられるようになっており、管理下にあるネットワークから攻撃者を輩出させないことも重要である。本研究の目的は、サービス拒否攻撃の中で最も用いられている攻撃の1つである SYN Flood 攻撃に着目し、小規模なネットワーク管理者に SYN Flood 攻撃の攻撃動向に関する情報を収集する手段を提供することである。</p> <p>従来、インターネット上の攻撃動向を早期に検知する手段として、インターネット観測システムが知られている。インターネット観測システムは、インターネット上に観測点と呼ばれる計算機を設置し、観測点に到着するパケットを捕捉・解析することで、インターネット上の脅威を早期に検知するためのシステムである。しかし、既存のインターネット観測システムの多くは、観測点の設置位置が固定されており、常に同じ設置位置での定点観測を行っている。近年では、攻撃者がこうした固定観測点の設置位置を事前に把握し、攻撃時に観測網を迂回する手法が発見されており、従来の固定観測点によるシステムの観測性能の低下が懸念されている。</p> <p>そこで筆者は、ネットワークセキュリティに関心を持った有志の小規模なネットワーク管理者が、インターネット上に P2P ネットワークを構築することでインターネット上の脅威である SYN Flood 攻撃を検出する手法を提案する。すなわち、各参加ノード自らが観測点となり、観測したパケットが保存されたネットワークログの情報を P2P ネットワークの参加ユーザ間で共有することで、インターネットの動的観測を実現する。また、各参加ノードが提供する攻撃情報の収集にはモバイルエージェントを採用している。</p> <p>本論文では、実際のインターネット上で取得されたネットワークログを評価実験に使用し、インターネット上の約 1/256 の状況を反映したシミュレーション評価を行った。</p> <p>最初に、調査対象とするネットワークログの調査時間範囲、誤検知を排除するための閾値設定の関係を明らかにするための評価実験を行った。これにより、誤検知を排除しつつ、より多くの SYN Flood 攻撃を検知するための各パラメータ調整についての議論を行った。また、特定の攻撃規模を想定した上で、攻撃の見逃しに関しても検証した。</p> <p>次に、従来の固定観測点による観測性能と本論文における動的観測点による観測性能との性能比較を行う。従来の固定観測点による攻撃観測は、検知性能の低下が懸念されていることはすでに述べた。しかしながら、ある特定の観測点が観測した攻撃動向の情報の質を、その観測点の検知性能として定量的に示す指標が存在していない。そこで、ある特定の観測点の検知性能を示す定量的な指標を定義する。そしてこの指標を基に、観測点が観測した攻撃動向の情報の質を数値化して評価することで、従来の固定観測点に対する本論文における動的観測点の優位性を示した。</p>
-------	--

孟 南	<p>ルーティングアルゴリズムによるセンサネットワークのセキュリティ強化手法に関する研究</p> <p>近年、センサネットワークが様々な分野に広く応用されるようになってきている。そのため、センサネットワークにおける情報漏洩の問題も重要視されるようになった。本研究はセンサノードから発信される電波を安全ではない領域外へ漏洩することをできるだけ抑えることにより、センサネットワークのセキュリティを向上させることを目的として、新しいルーティングアルゴリズムを提案する。シミュレーション実験により、既存手法との比較を行い、提案手法の優位性を確認した。</p>
-----	---

(分散システム講座(高田 II 研)に同じ)

(c) 博士(後期)論文概要

該当なし

(d) 講座所属学生が第一著者として査読ありの論文誌掲載論文一覧

該当なし

(e) 講座所属学生が各学会で登壇発表した実績一覧

- 1) Nan Meng, Jiahong Wang, Eiichiro Kodama, and Toyook Takata: Enhancing Sensor Network Security by Reducing Radio-Wave Leakage, Proc. 2011 International Workshop on Advances in Sensor Technologies, Systems and Applications (ASTSA-2011) in conjunction with 6th International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA-2011), Barcelona, Spain, October 26-28, 2011.
- 2) 孟 南, 王 家宏, 児玉 英一郎, 高田 豊雄: 電波漏洩の削減によるセンサネットワークのセキュリティ強化手法, 信学技報, NS, ネットワークシステム, Vol. 111, No. 196, NS2011-73, pp. 79-84, (Sept. 2011).
- 3) 孟 南, 王 家宏, 児玉 英一郎, 高田 豊雄: ルーティングアルゴリズムによるセンサネットワークのセキュリティ強化手法, 第 10 回情報科学技術フォーラム (Sept. 2011) (FIT ヤングリサーチャー賞, FIT の全論文件数の 1.5%) .
- 4) 小原 富美聡, ベッド B. ビスタ, 高田 豊雄: クラック困難なパスワードの作成を意識しないユーザでも利用可能な, 2 コマまんがを用いた認証方法の提案マルチタッチスクリーンを利用した認証方式の提案, コンピュータセキュリティシンポジウム 2011 (CSS2011) 論文集, pp.54-59 (Oct. 2011).
- 5) 成田 匡輝, ベッド B. ビスタ, 高田 豊雄: 動的観測点を利用した SYN Flood 攻撃検出手法とその有効性評価について, コンピュータセキュリティシンポジウム 2011 (CSS2011) 論文集, pp.558-563 (Oct. 2011).
- 6) 野地 脩宏, ベッド B. ビスタ, 高田 豊雄: 分散型インターネット観測システムにおけるモバイルエージェント移動戦略の提案, 信学技報, 人工知能と知識処理, Vol. 111, No. 310, AI2011-22, pp.31-36 (Nov. 2011).
- 7) 澤村 隆志, ベッド B. ビスタ, 高田 豊雄: PC 内のファイル改ざんを行うマルウェア検知手法の提案, 情報処理学会研究報告, Vol.2012-CSEC-56, No. 11, (7 ページ) (Feb. 2012).

(以上, 分散システム講座(高田 II 研)に同じ)

- 8) 吉田 優介, Bhed Bahadur Bista, 高田 豊雄: コミュニティ型サービスにおける個人情報の保護, 平成 23 年度電気関係学会 東北支部連合大会 講演論文集, p.135 (Aug. 2011).

(f) 学生が単独で受けた受賞や表彰一覧

孟南, FIT ヤングリサーチャー賞, ルーティングアルゴリズムによるセンサネットワークのセキュリティ強化手法(分散システム講座(高田 II 研)に同じ)